# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 2 |
| ***Control*** | Application/System Name/Title | ***Id Number*** | 6 |
| ***Guidance*** | Does the security plan identify the system consistently throughout the document and system lifecycle? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not identify the system consistently throughout the document. | | |
| ***Recommendation*** | NIST 800-18, section 3.2.1, recommends that the system be identified consistently throughout the document and system lifecycle. The eCB security plan identifies the system using numerous expressions. For example, the new Campus Based System, Campus Based, or CB system. The name of eCB should be consistent throughout the document. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 3 |
| ***Control*** | Assignment of Security Responsibility | ***Id Number*** | 11 |
| ***Guidance*** | Does the security plan identify an individual knowledgeable of management, operational, and technical controls used to protect system? If so, does this identification include<br>==> Name,<br>==> Title,<br>==> Organization,<br>==> Address, and<br>==> Phone number? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not identify the individual knowledgeable of management, operational, and technical controls used to protect system, and their title, organization, address, and phone number. | | |
| ***Recommendation*** | NIST 800-18, section 3.2.3, recommends that the security plan identify the individual knowledgeable of management, operational, and technical controls used to protect system and this information contain the individual's name, title, organization, address and phone number. The eCB security plan should contain a brief discussion of the sso's qualifications for the position. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 4 |
| ***Control*** | System Interconnection/Information Sharing | ***Id Number*** | 29 |
| ***Guidance*** | If there are any system interfaces, does the security plan reference written rules of behavior and controls for each of the interconnecting systems? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not have written rules of behavior and controls for each of the interconnecting systems. | | |
| ***Recommendation*** | NIST 800-18, section 3.6, recommends that the security plan reference written rules of behavior and controls for each of the interconnecting systems. Since eCB relies on other SFA systems and facilities, the security plan should maintain all relevant documentation from the interconnected systems security plans. At a minimum, the eCB SSO should reference the interconnected systems security plans, including appropriate version # and section # containing the applicable information. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 5 |
| ***Control*** | System Interconnection/Information Sharing | ***Id Number*** | 33 |
| ***Guidance*** | If there are any system interfaces, does the security plan include the type of interconnection for each interface? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not include a type of interconnection for each interface. | | |
| ***Recommendation*** | NIST 800-18, section 3.6, recommends that a security plan indicate the type of interconnection for each interface. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 6 |
| ***Control*** | System Interconnection/Information Sharing | ***Id Number*** | 34 |
| ***Guidance*** | If there are any system interfaces, does the security plan include a short discussion of major concerns/considerations for each interface? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not include a short discussion of major concerns/considerations for each interface. | | |
| ***Recommendation*** | NIST 800-18, section 3.6, recommends that a security plan include a short discussion of major concerns/considerations for each interface. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 7 |
| ***Control*** | System Interconnection/Information Sharing | ***Id Number*** | 35 |
| ***Guidance*** | If there are any system interfaces, does the security plan include the name and title of authorizing management official(s) for each interface? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not provide the name and title of the authorizing management official(s) for each system interface. | | |
| ***Recommendation*** | NIST 800-18, section 3.6, recommends that a security plan provide the name and title of the authorizing management official(s) for each system interface. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 8 |
| ***Control*** | System Interconnection/Information Sharing | ***Id Number*** | 36 |
| ***Guidance*** | If there are any system interfaces, does the security plan provide a date of authorization for each system interface? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not provide a date of authorization for each system interface. | | |
| ***Recommendation*** | NIST 800-18, section 3.6, recommends that a security plan provide a date of authorization for each system interface. Although SFA does not require formal authorization for interconnections between SFA systems, the date the systems were connected should be identified. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 9 |
| ***Control*** | System Interconnection/Information Sharing | ***Id Number*** | 37 |
| ***Guidance*** | If there are any system interfaces, does the security plan provide a statement indicating if the interfacing system is a "System of Record"? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not indicate if the interfacing system(s) are a "System of Record"? | | |
| ***Recommendation*** | NIST 800-18, section 3.6, recommends that a security plan indicate if the interfacing system(s) are a "System of Record"? | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 10 |
| ***Control*** | System Interconnection/Information Sharing | ***Id Number*** | 38 |
| ***Guidance*** | If there are any system interfaces, does the security plan describe the sensitivity level of each interconnected system? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the sensitivity level of each interconnected system. | | |
| ***Recommendation*** | NIST 800-18, section 3.6, recommends that a security plan describe the sensitivity level of each interconnected system. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 11 |
| ***Control*** | Sensitivity of Information Handled | ***Id Number*** | 252 |
| ***Guidance*** | Does the security plan specify that analysts and programmers were used to help design appropriate security controls for the system? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not indicate that analysts and programmers were used to help design appropriate security controls for the system? | | |
| ***Recommendation*** | NIST 800-18, section 3.7, recommends that a security plan indicate that analysts and programmers were used to help design appropriate security controls for the system. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 12 |
| ***Control*** | Laws, Regulations, and Policies Affecting the System | ***Id Number*** | 253 |
| ***Guidance*** | If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act system(s) of records and whether the system(s) are used for computer matching activities | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does indicate if the eCB system is a system of record, or if the system is used for computer matching activities. | | |
| ***Recommendation*** | NIST 800-18 recommends that a system identify if it is considered a system of record. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 13 |
| ***Control*** | Review of Security Controls | ***Id Number*** | 51 |
| ***Guidance*** | Does the security plan discuss the recommendations from the A-130 review including information concerning correction of deficiencies or completion of recommendations? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not discuss the recommendations from the A-130 review to include information concerning correction of deficiencies or completion of recommendations. | | |
| ***Recommendation*** | Upon completion of the risk assessment, the eCB security plan should include information concerning correction of deficiencies or completion of recommendations. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 14 |
| ***Control*** | Review of Security Controls | ***Id Number*** | 254 |
| ***Guidance*** | Indicate if the review identified a deficiency reportable under OMB A-123 or the Federal Managers' Financial Integrity Act if there is no assignment of security responsibility, no security plan, or no authorization to process for a system | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does contain language indicating deficiencies reportable under OMB A-123. | | |
| ***Recommendation*** | Upon completion of the risk assessment, the eCB security plan should contain language indicating deficiencies reportable under OMB A-123. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 15 |
| ***Control*** | Rules of Behavior | ***Id Number*** | 57 |
| ***Guidance*** | Does the rules of behavior include appropriate limits on:<br>==> interconnections to other systems,<br>==> work at home<br>==> dial-in access,<br>==> connection to Internet<br>==> use of copyrighted works<br>==> unofficial use of government equipment, and<br>==> individual accountability? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not defines matters such as work at home, dial-in access, connection to Internet, use of copyrighted works, unofficial use of government equipment, and individual accountability. | | |
| ***Recommendation*** | NIST 800-18, section 4.3, recommends that the Rules of Behavior for a system define matters such as work at home, dial-in access, connection to Internet, use of copyrighted works, unofficial use of government equipment, and individual accountability. The current rules of behavior correctly discusses numerous appropriate categories. However, the above issues should also be addressed. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 16 |
| ***Control*** | Rules of Behavior | ***Id Number*** | 59 |
| ***Guidance*** | Are the Rules of Behavior made available to the user prior to receiving authorization for access to the system? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not state that a Rules of Behavior are made available to the user prior to receiving authorization for access to the system. | | |
| ***Recommendation*** | NIST 800-18, section 4.3, recommends that a Rules of Behavior be made available to the user prior to receiving authorization for access to the system. The eCB security plan does indicate annual renewal of the rules of behavior document, but an additional statement should be included to indicate that users must sign the rules of behavior document prior to receiving access to eCB. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 17 |
| ***Control*** | Development/Acquisition Phase | ***Id Number*** | 63 |
| ***Guidance*** | If the system is in the development/acquisition phase of the life cycle, does the security plan document any specifications that were used during this phase? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not document the specifications that were used during the development/acquisition phase of the life cycle. | | |
| ***Recommendation*** | NIST 800-18, section 4.4.2, recommends that a security plan document the specifications that were used during the development/acquisition phase of the life cycle. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 18 |
| ***Control*** | Development/Acquisition Phase | ***Id Number*** | 64 |
| ***Guidance*** | If the system is in the development/acquisition phase of the life cycle, does the security plan document any security requirements that were used during this phase? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not document the specifications that were used during the development/acquisition phase of the life cycle. | | |
| ***Recommendation*** | NIST 800-18, section 4.4.2, recommends that a security plan document any security requirements that were used during the development/acquisition phase of the life cycle. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 19 |
| ***Control*** | Development/Acquisition Phase | ***Id Number*** | 65 |
| ***Guidance*** | If the system is in the development/acquisition phase of the life cycle, does the security plan document the test and evaluation procedures for security controls? Did the tests occur prior to procurement? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not document appropriate controls with associated evaluation and test procedures before the procurement action. | | |
| ***Recommendation*** | NIST 800-18, section 4.4.2, recommends that a security plan document appropriate controls with associated evaluation and test procedures before the procurement. When these procedures are available, they should be documented in the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 20 |
| ***Control*** | Development/Acquisition Phase | ***Id Number*** | 66 |
| ***Guidance*** | If the system is in the development/acquisition phase of the life cycle, does the security plan document if the solicitation documents included security requirements and evaluation/test procedures? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not document the security requirements in the solicitation document during the development/acquisition phase of the life cycle. | | |
| ***Recommendation*** | NIST 800-18, section 4.4.2, recommends that a security plan document the security requirements in the solicitation document during the development/acquisition phase of the life cycle. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 21 |
| ***Control*** | Development/Acquisition Phase | ***Id Number*** | 67 |
| ***Guidance*** | If the system is in the development/acquisition phase of the life cycle, does the security plan document the requirements permit updating the security requirements as new threats/vulnerabilities are identified and as new technologies are implemented during this phase? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not document the requirement to permit updating the security requirements as new threats/vulnerabilities are identified and as new technologies are implemented during this phase. | | |
| ***Recommendation*** | NIST 800-18, section 4.4.2, recommends that a security plan document the requirement to permit updating the security requirements as new threats/vulnerabilities are identified and as new technologies are implemented during this phase. A statement should be included to address new threats and vulnerabilities. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 22 |
| ***Control*** | Authorize Processing (Accreditation) | ***Id Number*** | 257 |
| ***Guidance*** | Does the security plan include the date of authorization, name, and title of management official? If the system is not authorized, does the security plan provide the name and title of manager requesting approval to operate and date of request? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not provide the date, name, and title of the management official authorizing the system for use. | | |
| ***Recommendation*** | NIST 800-18, section 4.5, recommends that a security plan provide the date, name, and title of the management official authorizing the system for use. Section 1.10 of the eCB security plan indicates that eCB will comply with FIPS 102, Certification and Accreditation. Therefore, a certification and accreditation process should be integrated as soon as possible. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 23 |
| ***Control*** | Authorize Processing (Accreditation) | ***Id Number*** | 258 |
| ***Guidance*** | Does the security plan state that a reauthorization is scheduled for every three years or upon major changes in the system? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not state that a reauthorization is scheduled every three years or upon major changes in the system. | | |
| ***Recommendation*** | NIST 800-18, section 4.5, recommends that a security plan state that a reauthorization is scheduled every three years or upon major changes in the system. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 24 |
| ***Control*** | Authorize Processing (Accreditation) | ***Id Number*** | 259 |
| ***Guidance*** | Does the security plan state that a technical and/or security evaluation was completed prior to authorizing the system for processing? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not state that a technical and/or security evaluation was completed prior to authorizing the system for processing. | | |
| ***Recommendation*** | NIST 800-18, section 4.5, recommends that a security plan state that a technical and/or security evaluation was completed prior to authorizing the system for processing. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 25 |
| ***Control*** | Personnel Controls - MA | ***Id Number*** | 80 |
| ***Guidance*** | Does the personnel security program integrate a Rules of Behavior document with their procedures? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not have personnel security procedures that integrate a Rules of Behavior document. | | |
| ***Recommendation*** | NIST 800-18, section 5.1, recommends that a security plan include information on how personnel security procedures integrate a Rules of Behavior document. This suggestion may occur, but is not documented in the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 26 |
| ***Control*** | Personnel Controls - MA | ***Id Number*** | 85 |
| ***Guidance*** | Does the security plan state that critical functions are divided among different individuals to ensure that no individual has all necessary authority or information access, which could result in fraudulent activity? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not require critical functions be separated among different individuals. | | |
| ***Recommendation*** | NIST 800-18, section 5.1, recommends that critical functions be separated among different individuals to ensure that no individual has all necessary authority or information access that could result in fraudulent activity. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 27 |
| ***Control*** | Personnel Controls - MA | ***Id Number*** | 88 |
| ***Guidance*** | Does the security plan describe the termination procedures for a friendly and an unfriendly termination? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the termination procedures for a friendly and an unfriendly termination. | | |
| ***Recommendation*** | NIST 800-18, section 5.1, recommends that a security plan describe the termination procedures for a friendly and an unfriendly termination. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 28 |
| ***Control*** | Physical and Environmental Protection - MA | ***Id Number*** | 95 |
| ***Guidance*** | If the system uses mobile or portable systems, does the security plan address how laptop computers are securely stored when they are not in use, and encrypt data files on stored media, when cost-effective, as a precaution against disclosure of information if a laptop is lost or stolen? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not address how laptop computers are securely stored when they are not in use. | | |
| ***Recommendation*** | NIST 800-18, section 5.2.1 recommends that a security plan address how laptop computers are securely stored when they are not in use, and encrypt data files on stored media, when cost-effective, as a precaution against disclosure of information if a laptop is lost or stolen. If eCB does not use laptops, this fact should be indicated in the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 29 |
| ***Control*** | Production, Input/Output Controls - MA | ***Id Number*** | 97 |
| ***Guidance*** | Does the security plan describe a help desk operation or group that offers advice? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe a help desk operation or group that offers advice. | | |
| ***Recommendation*** | NIST 800-18, section 5.3, recommends that a security plan describe a help desk operation or group that offers advice. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 30 |
| ***Control*** | Production, Input/Output Controls - MA | ***Id Number*** | 99 |
| ***Guidance*** | Does the security plan provide procedures to ensure only authorized personnel pick-up, receive, deliver input and output information and media? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the procedures to ensure only authorized personnel pick-up, receive, deliver input and output information and media | | |
| ***Recommendation*** | NIST 800-18, section 5.3, recommends that a security plan describe the procedures to ensure only authorized personnel pick-up, receive, deliver input and output information and media. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 31 |
| ***Control*** | Production, Input/Output Controls - MA | ***Id Number*** | 100 |
| ***Guidance*** | Does the security plan describe the audit trails for receipt of sensitive inputs/outputs? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the audit trails for receipt of sensitive inputs/outputs. | | |
| ***Recommendation*** | NIST 800-18, section 5.3, recommends that a security plan describe the audit trails for receipt of sensitive inputs/outputs. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 32 |
| ***Control*** | Production, Input/Output Controls - MA | ***Id Number*** | 102 |
| ***Guidance*** | Does the security plan describe the procedures and controls used for transporting or mailing media or printed output? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the procedures and controls used for transporting or mailing media or printed output. | | |
| ***Recommendation*** | NIST 800-18, section 5.3, recommends that a security plan describe the procedures and controls used for transporting or mailing media or printed output. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 33 |
| ***Control*** | Production, Input/Output Controls - MA | ***Id Number*** | 103 |
| ***Guidance*** | Does the security plan describe the internal and external labeling procedures? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the internal and external labeling procedures. | | |
| ***Recommendation*** | NIST 800-18, section 5.3, recommends that a security plan describe the internal and external labeling procedures. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 34 |
| ***Control*** | Production, Input/Output Controls - MA | ***Id Number*** | 104 |
| ***Guidance*** | Does the security plan describe the procedures for external labeling with special handling instructions? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the procedures for external labeling with special handling instructions. | | |
| ***Recommendation*** | NIST 800-18, section 5.3, recommends that a security plan describe the procedures for external labeling with special handling instructions. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 35 |
| ***Control*** | Production, Input/Output Controls - MA | ***Id Number*** | 105 |
| ***Guidance*** | Does the security plan describe the audit trails for inventory management? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the audit trails for inventory management. | | |
| ***Recommendation*** | NIST 800-18, section 5.3, recommends that a security plan describe the audit trails for inventory management. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 36 |
| ***Control*** | Production, Input/Output Controls - MA | ***Id Number*** | 106 |
| ***Guidance*** | Does the security plan describe the media storage vault or library physical environment protection controls and procedures? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the media storage vault or library physical environment protection controls and procedures. | | |
| ***Recommendation*** | NIST 800-18, section 5.3, recommends that a security plan describe the media storage vault or library physical environment protection controls and procedures. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 37 |
| ***Control*** | Production, Input/Output Controls - MA | ***Id Number*** | 107 |
| ***Guidance*** | Does the security plan describe the procedures for sanitizing electronic media for reuse? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the procedures for sanitizing electronic media for reuse. | | |
| ***Recommendation*** | NIST 800-18, section 5.3, recommends that a security plan describe the procedures for sanitizing electronic media for reuse | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 38 |
| ***Control*** | Production, Input/Output Controls - MA | ***Id Number*** | 108 |
| ***Guidance*** | Does the security plan mention procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not have procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse. | | |
| ***Recommendation*** | NIST 800-18, section 5.MA.3, recommends that there be procedures for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 39 |
| ***Control*** | Production, Input/Output Controls - MA | ***Id Number*** | 109 |
| ***Guidance*** | Procedures for shredding or other destructive measures for hardcopy media when no longer required | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not include procedures for hardcopy media when is no longer required. | | |
| ***Recommendation*** | The eCB security plan should include procedures for hardcopy media when is no longer required. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 40 |
| ***Control*** | Contingency Planning - MA | ***Id Number*** | 111 |
| ***Guidance*** | Are tested contingency plans in place to permit continuity of mission-critical functions in the event of a catastrophic event? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not include any testing information regarding contingency plans. | | |
| ***Recommendation*** | Contingency plans should be tested, generally, every year. The decision should be based on risk, the amount of change occurring within eCB or the supporting systems, or Departmental requirements. If the plans are tested, simply include a statement in the eCB security plan indicating this fact. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 41 |
| ***Control*** | Contingency Planning - MA | ***Id Number*** | 112 |
| ***Guidance*** | Are tested disaster recovery plans in place for all supporting IT systems and networks? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not indicate if all disaster recovery plans are in place and tested. | | |
| ***Recommendation*** | A testing schedule for disaster recovery plans should be documented in the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 42 |
| ***Control*** | Contingency Planning - MA | ***Id Number*** | 113 |
| ***Guidance*** | Does the security plan state that formal written emergency operating procedures are posted or located to facilitate their use in emergency situations? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not state that formal written emergency operating procedures be posted or located to facilitate their use in emergency situation | | |
| ***Recommendation*** | NIST 800-18, section 5.4, recommends that that formal written emergency operating procedures be posted or located to facilitate their use in emergency situation. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 43 |
| ***Control*** | Contingency Planning - MA | ***Id Number*** | 114 |
| ***Guidance*** | How often are contingency, disaster, and emergency plans tested? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe a testing schedule for contingency, disaster, and emergency plans. | | |
| ***Recommendation*** | A testing schedule for disaster recovery plans should be documented in the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 44 |
| ***Control*** | Application Software Maintenance Controls - MA | ***Id Number*** | 194 |
| ***Guidance*** | Does the government own the software? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not indicate ownership of the software. | | |
| ***Recommendation*** | The eCB security plan should contain a statement describing the ownership of the software used to operate and support eCB. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 45 |
| ***Control*** | Application Software Maintenance Controls - MA | ***Id Number*** | 195 |
| ***Guidance*** | Was the application software received from another federal agency with the understanding that it is federal government property? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not indicate if the software was received from another federal agency with the understanding that it is federal government property. | | |
| ***Recommendation*** | The eCB security plan should contain a statement describing the ownership of the software used to operate and support eCB, including if the software was received from another federal agency with the understanding that it is federal government property. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 46 |
| ***Control*** | Application Software Maintenance Controls - MA | ***Id Number*** | 196 |
| ***Guidance*** | Is the application software a copyrighted commercial off-the-self product or shareware? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not indicate if the software is a copyrighted commercial off-the-self product or shareware. | | |
| ***Recommendation*** | The eCB security plan should indicate the nature of the software, whether it is COTS, GOTS, etc. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 47 |
| ***Control*** | Application Software Maintenance Controls - MA | ***Id Number*** | 197 |
| ***Guidance*** | If a copyrighted commercial off-the-self product (or shareware), were sufficient licensed copies of the software purchased for all of the systems on which this application will be processed? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not indicate if the software is a copyrighted commercial off-the-self product or shareware. | | |
| ***Recommendation*** | The eCB security plan should indicate the nature of the software, whether it is COTS, GOTS, etc, and describe any established licensing agreements. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 48 |
| ***Control*** | Application Software Maintenance Controls - MA | ***Id Number*** | 201 |
| ***Guidance*** | Have trap door "hot keys" been activated for emergency data repairs? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the use of trap doors, or hot key for emergency repairs. | | |
| ***Recommendation*** | The eCB security plan should describe the use or lack of use of trap doors, or hot key for emergency repairs. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 49 |
| ***Control*** | Application Software Maintenance Controls - MA | ***Id Number*** | 204 |
| ***Guidance*** | Are there organizational policies against illegal use of copyrighted software or shareware? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe any organizational policies against illegal use of copyrighted software or shareware? | | |
| ***Recommendation*** | The eCB security plan should reference any SFA policies restricting the use of copyrighted software or shareware. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 50 |
| ***Control*** | Application Software Maintenance Controls - MA | ***Id Number*** | 206 |
| ***Guidance*** | What products and procedures are used to protect against illegal use of software? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe any products used to protect against illegal use of software. | | |
| ***Recommendation*** | NIST 800-18 recommends that a security plan state the products and procedures used to protect against illegal use of software. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 51 |
| ***Control*** | Data Integrity/ Validation Controls - MA | ***Id Number*** | 127 |
| ***Guidance*** | Is penetration testing performed on the system? If so, what procedures are in place to ensure they are conducted appropriately? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe penetration testing procedures. | | |
| ***Recommendation*** | NIST 800-18 recommends that penetration test be performed on the system and that there are procedures in place to ensure that it is conducted appropriately. The decision to use penetration tests should be based upon a risk-based decision. Some systems, due to their sensitivity level, do not require penetration tests. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 52 |
| ***Control*** | Data Integrity/ Validation Controls - MA | ***Id Number*** | 128 |
| ***Guidance*** | Is message authentication used in the application to ensure that the sender of a message is known and that the message has not been altered during a transmission? State whether a message authentication has been determined to be appropriate for your system. If so, describe methodology | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe message authentication procedures. | | |
| ***Recommendation*** | If applicable, message authentication procedures should be established to ensure that the sender of a message is known and that the message has not been altered during a transmission. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 53 |
| ***Control*** | Data Integrity/ Validation Controls - MA | ***Id Number*** | 210 |
| ***Guidance*** | Are password crackers/checkers used? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not indicate the use of password crackers/checkers. | | |
| ***Recommendation*** | NIST 800-18 recommends that password crackers be used against password files. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 54 |
| ***Control*** | Documentation - MA | ***Id Number*** | 140 |
| ***Guidance*** | Does the security plan provide detailed information on the systems user manuals? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not provide detailed information on the systems user manuals. | | |
| ***Recommendation*** | NIST 800-18, section 5.7, recommends that a security plan provide detailed information on the systems user manuals. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 55 |
| ***Control*** | Documentation - MA | ***Id Number*** | 143 |
| ***Guidance*** | Does the security plan provide detailed information on the systems authorize processing documents and statements? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not provide detailed information on the systems authorize processing documents and statements. | | |
| ***Recommendation*** | NIST 800-18, section 5.7, recommends that a security plan provide detailed information on the systems authorize processing documents and statements. These documents relate to the certification and accreditation process, which eCB has not formally initiated. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 56 |
| ***Control*** | Security Awareness and Training - MA | ***Id Number*** | 145 |
| ***Guidance*** | Does the security plan describe the type and frequency of application-specific training provided to employees and contractor personnel? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the type and frequency of application-specific training provided to employees and contractor personnel. | | |
| ***Recommendation*** | NIST 800-18, section 5.8, recommends that a security plan describe the type and frequency of application-specific training provided to employees and contractor personnel. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 57 |
| ***Control*** | Security Awareness and Training - MA | ***Id Number*** | 272 |
| ***Guidance*** | Does the security plan describe the type and frequency of general support system training provided to employees and contractor personnel? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the type and frequency of general support system training provided to employees and contractor personnel | | |
| ***Recommendation*** | NIST 800-18, section 5.8, recommends that a security plan describe the type and frequency of general support system training provided to employees and contractor personnel. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 58 |
| ***Control*** | Identification and Authentication - MA | ***Id Number*** | 158 |
| ***Guidance*** | Does the security plan describe procedures for eliminating Inactive User Ids | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe procedures for disabling accounts after a given period of inactivity | | |
| ***Recommendation*** | The eCB security plan should contain a statement describing procedures for disabling a user account after a given period of inactivity. The inactivity period should be defined in relation to acceptable level of risk and the Campus Based business cycle. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 59 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 219 |
| ***Guidance*** | Does the security plan identify whether the policies include separation of duties enforcement to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not identify whether system policies include separation of duties enforcement to prevent an individual from having all necessary authority or information access to allow fraudulent activity without collusion. | | |
| ***Recommendation*** | NIST 800-18, section 5.1, recommends that functional duties be separated to prevent fraudulent activity without collusion. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 60 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 220 |
| ***Guidance*** | Describe the application's capability to establish an Access Control List or register of the users and the types of access they are permitted. | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not contain language on access control lists. | | |
| ***Recommendation*** | NIST 800-18 recommends security plans contain a description of the application's capability to establish an Access Control List or register of the users and the types of access they are permitted. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 61 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 221 |
| ***Guidance*** | Does the security plan indicate whether a manual access control list is maintained for the system? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not state that a manual access control list is maintained for the system. | | |
| ***Recommendation*** | NIST 800-18, section 5.2, recommends that a manual access control list be maintained for the system. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 62 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 223 |
| ***Guidance*** | Describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties. | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties | | |
| ***Recommendation*** | NIST 800-18, section 5.MA.2, recommends that a security plan describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 63 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 224 |
| ***Guidance*** | Does the security plan indicate how often access control lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not indicate how often access control lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application. Procedures are established to remove users, but no mention of an access control list exists within the eCB security plan. | | |
| ***Recommendation*** | NIST 800-18, section 5.MA.2, recommends that a security plan indicate how often access control lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 64 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 226 |
| ***Guidance*** | Does the security plan describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users. | | |
| ***Recommendation*** | NIST 800-18, section 5.MA.2, recommends that a security plan describe policy or logical access controls that regulate how users may delegate access permissions or make copies of files or information accessible to other users. If users are not allowed to delegate their access permissions, this should be documented in the logical access section. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 65 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 228 |
| ***Guidance*** | Does the security plan describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not discuss the restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends. | | |
| ***Recommendation*** | NIST 800-18, section 6.MA.2, recommends that a security plan describe the restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends be discussed. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 66 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 229 |
| ***Guidance*** | Does the security plan indicate if encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures. | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not indicate if encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures. Encryption is used to ensure data integrity during data transmission. | | |
| ***Recommendation*** | NIST 800-18, section 6.MA.2, recommends that a security plan indicate if encryption is used to prevent unauthorized access to sensitive files as part of the system or application access control procedures. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 67 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 232 |
| ***Guidance*** | Provide information regarding any port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices, and if additional passwords or tokens are required. | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not provide information regarding port protection devices used to require specific access authorization to the communication ports, including the configuration of the port protection devices, and if additional passwords or tokens are required. | | |
| ***Recommendation*** | The eCB security plan should contain language describing port protection devices. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 68 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 233 |
| ***Guidance*** | Identify whether internal security labels are used to control access to specific information types or files, and if such labels specify protective measures or indicate additional handling instructions. | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not identify whether internal security labels are used to control access to specific information types or files, and if such labels specify protective measures or indicate additional handling instructions. | | |
| ***Recommendation*** | The eCB security plan should describe the labeling procedures employed to protect sensitive information. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 69 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 234 |
| ***Guidance*** | Does the security plan indicate if host-based authentication is used? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not indicate if host-based authentication is used | | |
| ***Recommendation*** | NIST 800-18, section 5.MA.2, recommends that a security plan state whether or not host based authentication is used. Host-based authentication is an access control approach that grants access based on the identity of the host originating the request, instead of the individual user requesting access. If eCB does not use this method of authentication, simply add a statement indicating this fact. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 70 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 236 |
| ***Guidance*** | Does the security plan state that a warning message is displayed, notifying unauthorized users that they have accessed a U.S. Government computer system and unauthorized use can be punished by fines or imprisonment. | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not have a standardized log-on banner notifying unauthorized users that they have accessed a U.S. Government computer system and unauthorized use can be punished by fines or imprisonment. | | |
| ***Recommendation*** | NIST 800-18, section 6.MA.2, recommends that a have a standardized log-on banner notifying unauthorized users that they have accessed a U.S. Government computer system and unauthorized use can be punished by fines or imprisonment. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 71 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 238 |
| ***Guidance*** | Does the security plan describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Department of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner. | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not have an approved warning banner displayed prior to login. | | |
| ***Recommendation*** | NIST 800-18, section 6.MA.2, recommends that an approved warning banner be displayed prior to login. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 72 |
| ***Control*** | Audit Trails - MA | ***Id Number*** | 183 |
| ***Guidance*** | Does the security plan state that audit trails are used as online tools to help identify problems other than intrusions as they occur? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not state that audit trails are used to help identify problems other than intrusions as they occur. | | |
| ***Recommendation*** | NIST 800-18, section 6.MA.4, recommends that a security plan state that audit trails are used to help identify problems other than intrusions as they occur. If the audit trails for eCB can be used for this function, simply add a statement stating this fact. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 73 |
| ***Control*** | Audit Trails - MA | ***Id Number*** | 186 |
| ***Guidance*** | Does the security plan state that there is a separation of duties between security personnel who administer the access control function and those who administer the audit trail? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not state that a separation of duties between security personnel who administer the access control function and those who administer the audit trail be described. | | |
| ***Recommendation*** | NIST 800-18, section 6.MA.2, recommends that a separation of duties between security personnel who administer the access control function and those who administer the audit trail be described. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 74 |
| ***Control*** | Audit Trails - MA | ***Id Number*** | 189 |
| ***Guidance*** | Does the security plan state that the audit trail be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not state that the application can query the audit trail by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information. | | |
| ***Recommendation*** | NIST 800-18, section 6.MA.2, recommends that the application be capable of querying the audit trail by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 75 |
| ***Control*** | Audit Trails - MA | ***Id Number*** | 191 |
| ***Guidance*** | Does the security plan state that audit analysis tools, such as those based on audit reduction, attack signature, and variance techniques, are used in a real-time or near real-time fashion. | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not have audit analysis tools based on audit reduction, attack signature, or variance techniques, are used in a real-time or near real-time fashion. | | |
| ***Recommendation*** | NIST 800-18, section 6.MA.4 recommends that audit analysis tools based on audit reduction, attack signature, or variance techniques, be used in a real-time or near real-time fashion. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 76 |
| ***Control*** | Audit Trails - MA | ***Id Number*** | 192 |
| ***Guidance*** | If keystroke monitoring is used, provide reference to the policy and the means of notification. Also indicate whether the DOJ has reviewed the policy. | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not indicate whether keystroke monitoring is used. | | |
| ***Recommendation*** | If keystroke monitoring is used in audit trails, organizations should have a written policy and notify users. The Rules of Behavior may be one vehicle for distributing the information. If keystroke monitoring is used, provide reference to the policy and the means of notification. Also indicate whether the Department of Justice has reviewed the policy. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 77 |
| ***Control*** | Authentication - MA | ***Id Number*** | 161 |
| ***Guidance*** | Does the security plan describe procedures for authentication specific training during its regularly scheduled training and awareness activities? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the inclusion of authentication into the security awareness and training section. | | |
| ***Recommendation*** | The eCB training and awareness program should include specific authentication training during its regularly scheduled training and awareness activities. Once this occurs, the training should be documented in the security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 78 |
| ***Control*** | Authentication - MA | ***Id Number*** | 168 |
| ***Guidance*** | Does the security plan describe the self-protection techniques for the user authentication mechanism? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the self-protection techniques for the user authentication mechanism. | | |
| ***Recommendation*** | NIST 800-18, section 6.MA.1.2, recommends that a security plan describe the self-protection techniques for the user authentication mechanism. (e.g., passwords are transmitted and stored with one-way encryption to prevent anyone [including the System Administrator] from reading the clear-text PIN number and associated information. If there are self-protection techniques employed, identify this in the authentication section of the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 79 |
| ***Control*** | Authentication - MA | ***Id Number*** | 169 |
| ***Guidance*** | State the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) and describe the actions taken when that limit is exceeded. | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not state the number of invalid access attempts that may occur for a given user identifier or access location (terminal or port) or describe the actions taken when that limit is exceeded | | |
| ***Recommendation*** | The eCB security plan should establish procedures to account for invalid access attempts. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 80 |
| ***Control*** | Authentication - MA | ***Id Number*** | 170 |
| ***Guidance*** | Describe the procedures for verifying that all system-provided administrative default passwords have been changed | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the procedures for verifying that all system-provided administrative default passwords have been changed | | |
| ***Recommendation*** | The eCB security plan should indicate procedures for ensuring default passwords have been changed. This issue may need to be discussed with VDC personnel. If the VDC personnel claim they have these controls, make sure to obtain the version number, date, and point of contact of the document that contains this information. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 81 |
| ***Control*** | Authentication - MA | ***Id Number*** | 171 |
| ***Guidance*** | Describe the security plan describe procedures for limiting scripts with embedded passwords. | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not have procedures for limiting scripts with embedded passwords. | | |
| ***Recommendation*** | NIST 800-18, section 6.MA.1.2, recommends that a security plan have procedures for limiting scripts with embedded passwords. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 82 |
| ***Control*** | Authentication - MA | ***Id Number*** | 172 |
| ***Guidance*** | Does the security plan describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies and any compensating controls? | | |
| ***Status*** | Not Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies and any compensating controls | | |
| ***Recommendation*** | NIST 800-18, section 6.MA.1.2, recommends that a security plan describe any policies that provide for bypassing user authentication requirements, single-sign-on technologies and any compensating controls. If none exist, state this in the authentication section of the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 83 |
| ***Control*** | System Boundary Description | ***Id Number*** | 239 |
| ***Guidance*** | Does the system security plan describe the system's boundary to including<br>==>management control,<br>==>interconnections,<br>==>operating characteristics, and<br>==>mission objective. | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not specifically describe the system boundary. The plan describes numerous components of the system boundary, such as interconnections and mission objective, but does not organize the information into a system boundary section. | | |
| ***Recommendation*** | NIST 800-18 recommends the system security plan contain a section specifically describing the system's boundary. Ideally, the section would describe a logical and physical diagram of the system, the interconnections with other sections, any pertinent operating characteristics, and the overall mission objective. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 84 |
| ***Control*** | Assignment of Security Responsibility | ***Id Number*** | 10 |
| ***Guidance*** | Does the security plan identify an individual who is assigned security responsibility and is this assignment in writing containing:<br>==> Name,<br>==> Title,<br>==> Organization,<br>==> Address, and<br>==> Phone number? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not identify the system security officer responsibility in an attached written assignment letter. | | |
| ***Recommendation*** | NIST 800-18, section 3.2.4, recommends that the security plan identify a system security officer, that their responsibility be in writing and that the plan include their name, title, organization, address, and phone number. The system manager of eCB should assign, in writing, a system security officer. The letter should be attached to the security plan and be maintained by the SSO. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 85 |
| ***Control*** | General Description/ Purpose | ***Id Number*** | 16 |
| ***Guidance*** | Does the security plan provide a one to three paragraph description of function and purpose of system? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 1.7 of the eCB security plan dated September 13, 2001 does provide a one to three paragraph description of function and purpose of system. | | |
| ***Recommendation*** | NIST 800-18, section 3.4, recommends that a security plan provide a one to three paragraph description of function and purpose of system. The General Description/Purpose section should provide somewhat more detail as to the business process the eCB supports. Currently, this section in the eCB security plan discusses user privileges with only one sentence describing the general purpose of the system. A business process diagram may also be beneficial in this section. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 86 |
| ***Control*** | Application/System Environment | ***Id Number*** | 23 |
| ***Guidance*** | Does the security plan discuss the type of communications used by the application? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 1.8 of the eCB security plan dated September 13, 2001 does discuss the type of communications used by the application. | | |
| ***Recommendation*** | NIST 800-18, section 3.5, recommends that a security plan discuss the type of communications used by the application. The technical architecture diagram depicts the connection of eCB to its business partners through the internet. However, more detail should provided pertaining to this connection due to its inherent risk. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 87 |
| ***Control*** | Application/System Environment | ***Id Number*** | 24 |
| ***Guidance*** | Does the security plan describe the controls used to protect communication lines? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 1.8 of the eCB security plan dated September 13, 2001 does describe the controls used to protect communication lines. | | |
| ***Recommendation*** | NIST 800-18 recommends that the security plan describe the controls used to protect communication lines, as far as encryption. However, no physical security controls that protect the communication lines are described. A solution to this issue may be to reference the VDC as the responsible party for physical protection of the communication lines. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 88 |
| ***Control*** | Application/System Environment | ***Id Number*** | 246 |
| ***Guidance*** | Is it located in a harsh or overseas environment? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 1.8 of the eCB security plan dated September 13, 2001 does identify the location of the system | | |
| ***Recommendation*** | The eCB security plan is located at the VDC. However, the plan should also indicate that the VDC is located in Meriden, CT. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 89 |
| ***Control*** | System Interconnection/Information Sharing | ***Id Number*** | 28 |
| ***Guidance*** | If there are any system interfaces, does the security plan reflect written management authorization being obtained prior to connecting with other systems and/or sharing sensitive data/information ? Is there a list of interconnected systems including the Internet? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not have a written management authorization for system interfaces. | | |
| ***Recommendation*** | NIST 800-18, section 3.6, recommends that a written management authorization be obtained prior to connecting with other systems and/or sharing sensitive data/information. However, SFA policy does not require interconnection agreements between SFA systems. This should be indicated in the security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 90 |
| ***Control*** | System Interconnection/Information Sharing | ***Id Number*** | 32 |
| ***Guidance*** | If there are any system interfaces, does the security plan include the name of the organizations owning the other systems? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not identify the organization(s) owning the interfaced systems. | | |
| ***Recommendation*** | NIST 800-18, section 3.6, recommends that the security plan identify the organizations owning the interfaced systems. The eCB security plan references the name of the system, but does not reference the controlling organization. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | System Identification | ***Finding Number*** | 91 |
| ***Control*** | Sensitivity of Information Handled | ***Id Number*** | 42 |
| ***Guidance*** | Does the security plan mention internal and external auditors evaluating the system security measures? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 2.3 of the eCB security plan dated September 13, 2001 does describe the results of an internal and external audit which evaluates the system security measures. | | |
| ***Recommendation*** | NIST 800-18, section 3.7, recommends that a security plan describe the results of an internal and external audit which evaluates the system security measures. The eCB security mentions an audit function, but does not describe the findings of any previous audits. eCB is scheduled to have a risk assessment completed during November 2001. The findings from this assessment should be included in the security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Plan Development | ***Finding Number*** | 92 |
| ***Control*** | Plan Control | ***Id Number*** | 2 |
| ***Guidance*** | The federal organizational sub-component responsible for the system, its physical location and address (if applicable, both local/state/contractor and federal org with description of relationship) | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 1.3 of the eCB security plan dated September 13, 2001 does list the federal organizational sub-component responsible for the system, but not its physical location and address. | | |
| ***Recommendation*** | NIST 800-18, section 3.2, recommends that security plans list the federal organizational sub-component responsible for the system, its physical location and address. eCB should document the physical location and address of SFA and/or the eCB office if located separately from SFA. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 93 |
| ***Control*** | Risk Assessment and Management | ***Id Number*** | 47 |
| ***Guidance*** | Does the security plan provide a one paragraph description of the value of the system or application, threats, vulnerabilities, and effectiveness of current or proposed safeguards? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the value of the system or application, threats, vulnerabilities, and effectiveness of current or proposed safeguards. | | |
| ***Recommendation*** | NIST 800-18, section 3.7.2, recommends that a security plan describe the value of the system or application, threats, vulnerabilities, and effectiveness of current or proposed safeguards. A risk assessment currently is being conducted that will identify threats, vulnerabilities, and effectiveness of the current and proposed safeguards. The findings from the risk assessment should be documented in the security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 94 |
| ***Control*** | Review of Security Controls | ***Id Number*** | 50 |
| ***Guidance*** | Does the security plan discuss the previous A-130 review(s) and finding(s) conducted on the system describing<br><br>==> Who conducted the review, and<br>==> The findings of the review? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 2.1 of the eCB security plan dated September 13, 2001 does identify who conducted the A-130 review. | | |
| ***Recommendation*** | NIST 800-18, section 4.2, recommends that a security plan identify who conducted the A-130 review and the findings of the review. When the risk assessment is completed, all findings should be documented in the security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 95 |
| ***Control*** | Rules of Behavior | ***Id Number*** | 54 |
| ***Guidance*** | Does the Rules of Behavior clearly delineate responsibilities and expected behavior of all individuals with access to system? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 2.3 of the eCB security plan dated September 13, 2001 does delineate responsibilities and expected behavior of a general user class with system access to system in the Rules of Behavior document. | | |
| ***Recommendation*** | NIST 800-18, section 4.3, recommends that a Rules of Behavior clearly delineate responsibilities and expected behavior of all individuals with access to system. The eCB security plan should specifically delineate each user class, from network engineer to desktop user and indicate their responsibilities when accessing the system. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 96 |
| ***Control*** | Rules of Behavior | ***Id Number*** | 56 |
| ***Guidance*** | Does that security plan state that the Rules of Behavior are in writing and form the basis for security awareness and training? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 2.3 of the eCB security plan dated September 13, 2001 does state the Rules of Behavior are in writing but do not mention the rules of behavior form the basis for security awareness and training. | | |
| ***Recommendation*** | NIST 800-18, section 4.3, recommends that the Rules of Behavior are in writing and form the basis for security awareness and training. The eCB security plan should include a statement indicating that the rules of behavior will form the basis for security awareness and training. This statement will further demonstrate the importance of knowing and understanding the rules of behavior to the signee. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 97 |
| ***Control*** | Rules of Behavior | ***Id Number*** | 58 |
| ***Guidance*** | Does the Rules of Behavior reflect the administrative and technical security controls in the system? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 2.3 of the eCB security plan dated September 13, 2001 does address administrative and technical security controls in the system. | | |
| ***Recommendation*** | Additional information should be added to describe the correlation between the policy and the actual security control affected by that policy. For example, rules regarding password use should be consistent with technical password features in the system. Such rules would also include limitations on changing information, searching databases, or divulging information. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 98 |
| ***Control*** | Authorize Processing (Accreditation) | ***Id Number*** | 260 |
| ***Guidance*** | Does the security plan state that a risk assessment must be conducted prior to authorizing a system for processing? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 2.1 of the eCB security plan dated September 13, 2001 does indicate that a risk assessment will be conducted, but does not mention its timing with the authorization of the system. | | |
| ***Recommendation*** | NIST 800-18 requires that a Risk Assessment be conducted prior to authorization for system processing. A statement should be added in the C&A section indicating this suggestion. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 99 |
| ***Control*** | Authorize Processing (Accreditation) | ***Id Number*** | 262 |
| ***Guidance*** | Does the security plan state that a contingency plan must be developed and tested prior to authorizing a system for processing? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.4 of the eCB security plan dated September 13, 2001 does include a description of the contingency planning for eCB and associated facilities. | | |
| ***Recommendation*** | NIST 800-18 recommends that a contingency plan be tested prior to authorizing a system for processing. No information about the authorization of the system was given. If a date of authorization exists, or is pending, indicate this in the C&A section. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 100 |
| ***Control*** | Authorize Processing (Accreditation) | ***Id Number*** | 264 |
| ***Guidance*** | System must meet all applicable federal laws, regulations, policies, guidelines, and standards prior to authorizing a system for processing | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 1.10 of the eCB security plan dated September 13, 2001 does list all applicable federal laws, regulations, policies, guidelines, and standards, but does not mention the date of authorization for the system | | |
| ***Recommendation*** | No information about the authorization of the system was given. If a date of authorization exists, or is pending, indicate this in the C&A section. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | Management Controls | ***Finding Number*** | 101 |
| ***Control*** | Authorize Processing (Accreditation) | ***Id Number*** | 265 |
| ***Guidance*** | In-place and planned security safeguards must appear to be adequate and appropriate for the system prior to authorizing a system for processing | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 1.8 of the eCB security plan dated September 13, 2001 does include a description of security safeguards. | | |
| ***Recommendation*** | A certification and accreditation program should be established. Once established a formal determination as to the adequacy of existing and planned security safeguards can be addressed. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 102 |
| ***Control*** | Personnel Controls - MA | ***Id Number*** | 83 |
| ***Guidance*** | Does the security plan identify whether individuals are permitted system access prior to completion of appropriate background screening? If individuals are permitted access to the system prior to completion of appropriate background screening, does the security plan describe conditions under which this is allowed and any compensating controls to mitigate associated risk? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not identify whether individuals are permitted system access prior to completion of appropriate background screening. | | |
| ***Recommendation*** | NIST 800-18, section 5.1, recommends that a security plan identify whether individuals are permitted system access prior to completion of appropriate background screening. The eCB security plan identifies the access revocation procedures, but does not indicate if a user can gain access to the system prior to the investigation's completion. A simple statement indicating this suggestion is sufficient. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 103 |
| ***Control*** | Physical and Environmental Protection - MA | ***Id Number*** | 89 |
| ***Guidance*** | Does the security plan address the physical access control measures in place? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.2 of the eCB security plan dated September 13, 2001 references the VDC as the provider of physical security. | | |
| ***Recommendation*** | The eCB security plan should reference the VDC security plan, its version number, and the section within the plan that discusses this control area. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 104 |
| ***Control*** | Physical and Environmental Protection - MA | ***Id Number*** | 90 |
| ***Guidance*** | Does the security plan describe the fire safety devices of the buildings that house the systems? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not describe the fire safety devices of the buildings that house the systems. | | |
| ***Recommendation*** | The eCB security plan should reference the VDC security plan, its version number, and the section within the plan that discusses this control area. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 105 |
| ***Control*** | Physical and Environmental Protection - MA | ***Id Number*** | 91 |
| ***Guidance*** | Does the security plan address the failure of supporting utilities including failures of electric power, heating and air-conditioning systems, water, sewage, and other utilities? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not address the failure of supporting utilities including electric power, heating and air-conditioning systems, water, sewage, and others. | | |
| ***Recommendation*** | The eCB security plan should reference the VDC security plan, its version number, and the section within the plan that discusses this control area. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 106 |
| ***Control*** | Physical and Environmental Protection - MA | ***Id Number*** | 92 |
| ***Guidance*** | Does the security plan address the procedures and plans to be followed in the event of a structural collapse? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not address the procedures and plans to be followed in the event of a structural collapse. | | |
| ***Recommendation*** | The eCB security plan should reference the VDC security plan, its version number, and the section within the plan that discusses this control area. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 107 |
| ***Control*** | Physical and Environmental Protection - MA | ***Id Number*** | 93 |
| ***Guidance*** | Does the security plan address the procedures and plans to be followed in the event of a plumbing leak? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not address the procedures and plans to be followed in the event of a plumbing leak. | | |
| ***Recommendation*** | The eCB security plan should reference the VDC security plan, its version number, and the section within the plan that discusses this control area. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 108 |
| ***Control*** | Physical and Environmental Protection - MA | ***Id Number*** | 94 |
| ***Guidance*** | Does the security plan address the procedures and plans to be followed if data is intercepted? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not address the procedures and plans to be followed if data is intercepted? | | |
| ***Recommendation*** | The eCB security plan should reference the VDC security plan, its version number, and the section within the plan that discusses this control area. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 109 |
| ***Control*** | Production, Input/Output Controls - MA | ***Id Number*** | 98 |
| ***Guidance*** | Does the security plan provide procedures to ensure unauthorized users cannot read, copy, alter, and steal printed or electronic information? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.6 of the eCB security plan dated September 13, 2001 does provide a limited description of procedures to ensure unauthorized users cannot read, copy, alter, steal printed or electronic information. | | |
| ***Recommendation*** | NIST 800-18, section 5.3, recommends that a security plan provide procedures to ensure unauthorized users cannot read, copy, alter, and steal printed or electronic information. A more detailed description of these procedures should be included in the input/output controls section, and related to section 3.6 of the eCB security plan (Data Integrity). | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 110 |
| ***Control*** | Production, Input/Output Controls - MA | ***Id Number*** | 101 |
| ***Guidance*** | Does the security plan describe the procedures for restricting access to input and output products? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.3 of the eCB security plan dated September 13, 2001 does describe the audit trails for receipt of sensitive inputs and outputs. | | |
| ***Recommendation*** | NIST 800-18, section 5.3, recommends that a security plan describe the audit trails for receipt of sensitive inputs and outputs. The eCB security plan references SAIG enrollment procedures for restricting access. These procedures should either be described in detail in this plan or the SAIG security plan should be referenced, including version number, section number, and contact information of the document controller. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 111 |
| ***Control*** | Contingency Planning - MA | ***Id Number*** | 110 |
| ***Guidance*** | Describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable and provide detailed plans as an attachment | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.4 of the eCB security plan dated September 13, 2001 refers to CSC documentation for the contingency plan information. | | |
| ***Recommendation*** | The eCB security plan should provide additional information for the contingency plan section. For example, eCB relies on other parties (VDC) to respond to contingencies and disasters. Therefore, the eCB security plan should include the version number, date, section and point of contact information for every document eCB will rely on in the event of an emergency. Another alternative is to maintain a copy of the VDC/CSC documentation with the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 112 |
| ***Control*** | Contingency Planning - MA | ***Id Number*** | 116 |
| ***Guidance*** | Does the security plan provide a description of any agreements for backup processing? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.4 of the eCB security plan dated September 13, 2001 does refer to other documentation containing this information. | | |
| ***Recommendation*** | NIST 800-18, section 5.4, recommends that a security plan provide a description of any agreements for backup processing. If the eCB security plan relies on support systems/personnel for this function, the eCB security plan should describe the version number, date, and section number of the document containing this information. Also, the person in charge of the supporting documentation should be identified in the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 113 |
| ***Control*** | Contingency Planning - MA | ***Id Number*** | 117 |
| ***Guidance*** | Does the security plan Documented backup procedures including frequency (daily, weekly, monthly) and scope (full backup, incremental backup, and differential backup)? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.4 of the eCB security plan dated September 13, 2001 does refer to other documentation containing this information. | | |
| ***Recommendation*** | NIST 800-18, section 5.4, recommends that a security plan document backup procedures. If the eCB security plan relies on support systems/personnel for this function, the eCB security plan should describe the version number, date, and section number of the document containing this information. Also, the person in charge of the supporting documentation should be identified in the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 114 |
| ***Control*** | Contingency Planning - MA | ***Id Number*** | 118 |
| ***Guidance*** | Discuss the security plan address the location of stored backups (off-site or on-site) | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.4 of the eCB security plan dated September 13, 2001 does refer to other documentation containing this information. | | |
| ***Recommendation*** | NIST 800-18, section 5.4, recommends that a security plan document the location of stored backups. If the eCB security plan relies on support systems/personnel for this function, the eCB security plan should describe the version number, date, and section number of the document containing this information. Also, the person in charge of the supporting documentation should be identified in the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 115 |
| ***Control*** | Contingency Planning - MA | ***Id Number*** | 119 |
| ***Guidance*** | Does the security plan address the generation of system backups? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.4 of the eCB security plan dated September 13, 2001 does refer to other documentation containing this information. | | |
| ***Recommendation*** | NIST 800-18, section 5.4, recommends that a security plan document procedures for generating backups. If the eCB security plan relies on support systems/personnel for this function, the eCB security plan should describe the version number, date, and section number of the document containing this information. Also, the person in charge of the supporting documentation should be identified in the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 116 |
| ***Control*** | Application Software Maintenance Controls - MA | ***Id Number*** | 198 |
| ***Guidance*** | Is there a formal change control process in place for the application, and if so, does it require that all changes to the application software be tested and approved before being put into production? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.5 of the eCB security plan dated September 13, 2001 does refer to an eCB configuration management plan. | | |
| ***Recommendation*** | The configuration management plan should either be included with the eCB security plan as an attachment, or the precise version number, date, and POC for the document controller should be identified in section 3.5 of the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 117 |
| ***Control*** | Application Software Maintenance Controls - MA | ***Id Number*** | 205 |
| ***Guidance*** | Does the security plan describe periodic audits of users' computers (PCs) to ensure only legally licensed copies of software are installed? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 4.4 of the eCB security plan dated September 13, 2001 does describe continual auditing of individual accounts. | | |
| ***Recommendation*** | NIST 800-18, section 5.5, recommends that periodic audits be conducted on users computers (PCs) to ensure only legally licensed copies of software is installed. While it is important to maintain audit logs of individual activity, it is also critical to routinely audit these logs. Once this procedure is established, document it in the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 118 |
| ***Control*** | Data Integrity/ Validation Controls - MA | ***Id Number*** | 126 |
| ***Guidance*** | Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.6 of the eCB security plan dated September 13, 2001 does describe a security tool called tripwire, which is used for system monitoring. | | |
| ***Recommendation*** | A more detailed description of tripwire's functionality should be included in the eCB security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 119 |
| ***Control*** | Data Integrity/ Validation Controls - MA | ***Id Number*** | 208 |
| ***Guidance*** | Is virus detection and elimination software installed? If so, are there procedures for: Updating virus signature files; Automatic and/or manual virus scans (automatic scan on network log-in, automatic scan on client/server power on, automatic scan on disk? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.6 of the eCB security plan dated September 13, 2001 does indicate the use of Virus Scan NT, Version 4.0.3A. However, no procedures exist for updating virus signature files. | | |
| ***Recommendation*** | NIST 800-18 recommends that virus scanners be used and that there are procedures in place to automatically update the signature database. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 120 |
| ***Control*** | Data Integrity/ Validation Controls - MA | ***Id Number*** | 212 |
| ***Guidance*** | Are intrusion detection tools installed on the system? Describe where the tool(s) are placed, the type of processes detected/reported, and the procedures for handling intrusions. (Reference Section 5.MA.3 Production, Input/Output Controls if the procedure | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.6 of the eCB security plan dated September 13, 2001 does describe the use of TRIPWIRE as an intrusion detection device. However, no details regarding where the tool(s) are placed, the type of processes detected/reported, and the procedures for handling intrusions are described. | | |
| ***Recommendation*** | The eCB security plan should describe the details regarding where the tool(s) are placed, the type of processes detected/reported, and the procedures for handling intrusions. Also, a logical and physical diagram of the intrusion detection architecture/design should accompany the description. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 121 |
| ***Control*** | Documentation - MA | ***Id Number*** | 131 |
| ***Guidance*** | Does the security plan provide detailed information on the systems Vendor-supplied documentation of hardware | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.7 of the eCB security plan dated September 13, 2001 does indicate that Vendor-supplied documentation of hardware is maintained. | | |
| ***Recommendation*** | NIST 800-18, section 5.7 recommends that a security plan not only indicate that this information is maintained, but also include this information with the Security plan. If the information is maintained in another document, identify the name of the document, its version number, and the section where the identified information is located. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 122 |
| ***Control*** | Documentation - MA | ***Id Number*** | 132 |
| ***Guidance*** | Does the security plan provide detailed information on the systems Vendor-supplied documentation of software? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.7 of the eCB security plan dated September 13, 2001 does indicate that Vendor-supplied documentation of software is maintained. | | |
| ***Recommendation*** | NIST 800-18, section 5.7 recommends that a security plan not only indicate that this information is maintained, but also include this information with the Security plan. If the information is maintained in another document, identify the name of the document, its version number, and the section where the identified information is located. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 123 |
| ***Control*** | Documentation - MA | ***Id Number*** | 133 |
| ***Guidance*** | Does the security plan provide detailed information on the systems General support system security plan? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not include detailed information on the system's General Support System security plan. | | |
| ***Recommendation*** | NIST 800-18, section 5.7 recommends that a security plan document or specifically refer to the security plan of the General Support System supporting the system. The VDC does not currently have a security plan. However, this fact should be noted and a date when the VDC security plan will be finished should be documented. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 124 |
| ***Control*** | Documentation - MA | ***Id Number*** | 134 |
| ***Guidance*** | Does the security plan provide detailed information on the systems Testing procedures and results? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not provide detailed information on the system's testing procedures and results. The security plan refers to the eCB configuration plan. | | |
| ***Recommendation*** | NIST 800-18, section 5.7 recommends that a security plan contain an appropriate level of detail describing the testing procedures and results. If the configuration management plan does contain this detail, the eCB security plan should reference the document specifically including the date, version number and section number describing the test results and procedures. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 125 |
| ***Control*** | Documentation - MA | ***Id Number*** | 135 |
| ***Guidance*** | Does the security plan provide detailed information on the systems standard operating procedures? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.7 of the eCB security plan dated September 13, 2001 does reference documentation for the system's standard operating procedures. | | |
| ***Recommendation*** | NIST 800-18, section 5.7 recommends that a security plan not only indicate that this information is maintained, but also include this information with the Security plan. If the information is maintained in another document, identify the name of the document, its version number, and the section where the identified information is located. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 126 |
| ***Control*** | Documentation - MA | ***Id Number*** | 136 |
| ***Guidance*** | Does the security plan provide detailed information on the systems emergency procedures? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.7 of the eCB security plan dated September 13, 2001 does reference documentation maintained on the system's emergency procedures. | | |
| ***Recommendation*** | NIST 800-18, section 5.7, recommends that a security plan not only indicate that this information is maintained, but also include this information with the Security plan. If the information is maintained in another document, identify the name of the document, its version number, and the section where the identified information is located. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 127 |
| ***Control*** | Documentation - MA | ***Id Number*** | 137 |
| ***Guidance*** | Does the security plan provide detailed information on the systems contingency plan? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.7 of the eCB security plan dated September 13, 2001 does reference documentation for a contingency plan currently under development. | | |
| ***Recommendation*** | NIST 800-18, section 5.7, recommends that a security plan not only indicate that this information is maintained, but also include this information with the Security plan. If the information is maintained in another document, identify the name of the document, its version number, and the section where the identified information is located. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 128 |
| ***Control*** | Documentation - MA | ***Id Number*** | 138 |
| ***Guidance*** | Does the security plan provide detailed information on the systems disaster recovery plans? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.4 of the eCB security plan dated September 13, 2001 does indicate that a disaster recovery plan is in place. However, no mention of documentation exists in the eCB security plan. | | |
| ***Recommendation*** | NIST 800-18, section 5.7, recommends that a security plan provide detailed information on the systems disaster recovery plans. The eCB security plan should not only indicate that this information is maintained, but also include this information with the Security plan. If the information is maintained in another document, identify the name of the document, its version number, and the section where the identified information is located. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 129 |
| ***Control*** | Documentation - MA | ***Id Number*** | 141 |
| ***Guidance*** | Does the security plan provide detailed information on the systems risk assessment? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 2.1 of the eCB security plan dated September 13, 2001 does provide information on the system's risk assessment. | | |
| ***Recommendation*** | NIST 800-18, section 5.7, recommends that a security plan provide detailed information on the systems risk assessment. eCB is currently undergoing a risk assessment. Upon completion of the assessment, the eCB security plan should be updated with the findings. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 130 |
| ***Control*** | Documentation - MA | ***Id Number*** | 142 |
| ***Guidance*** | Does the security plan provide detailed information on the systems backup procedures? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.4 of the eCB security plan dated September 13, 2001 does provide information on the systems backup procedures. However, the detail recommended was not provided. | | |
| ***Recommendation*** | NIST 800-18, section 5.7, recommends that a security plan not only indicate that this information is maintained, but also include this information with the Security plan. If the information is maintained in another document, identify the name of the document, its version number, and the section where the identified information is located. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 131 |
| ***Control*** | Documentation - MA | ***Id Number*** | 271 |
| ***Guidance*** | Does the Security Plan document Memoranda of understanding with interfacing systems? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | The eCB security plan dated September 13, 2001 does not include a copy of the memoranda of understanding with interfacing systems. | | |
| ***Recommendation*** | NIST 800-18 recommends that a Rules of Behavior, MOU, or MOA be prepared for each interface prior to interconnecting systems. The eCB security plan does mention the existence of the MOUs but does not include them with the security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Operational Controls | ***Finding Number*** | 132 |
| ***Control*** | Security Awareness and Training - MA | ***Id Number*** | 146 |
| ***Guidance*** | Does the security plan describe the procedures for assuring that employees and contractor personnel have been provided adequate training? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 3.8 of the eCB security plan dated September 13, 2001 does describe the need for contractors and employees to obtain security awareness and training. However, the security plan does not describe the procedures for assuring that employees and contractor personnel have been provided adequate training. | | |
| ***Recommendation*** | NIST 800-18, section 5.8, recommends that a security plan describe the procedures for assuring that employees and contractor personnel have been provided adequate training. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 133 |
| ***Control*** | Identification and Authentication - MA | ***Id Number*** | 155 |
| ***Guidance*** | Does the security plan address unique identification of users accessing the system? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 4.1 of the eCB security plan dated September 13, 2001 does describe the unique identification methods used by eCB. A unique PIN is assigned to each user and a school-based TG number is used to complete the identification. | | |
| ***Recommendation*** | The eCB security plan does not indicate the controls used to ensure the PIN is not shared at the client's site. A statement in the eCB security plan should be added to address this issue. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 134 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 177 |
| ***Guidance*** | Discuss controls in place to authorize or restrict the activities of users and system personnel within the application. | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 4.2 of the eCB security plan dated September 13, 2001 does describe controls in place to restrict the activities of users within the application. The plan describes a 20-minute time out period, restricting access to the system after a period of inactivity. | | |
| ***Recommendation*** | The eCB security plan should describe the controls in place to authorize or restrict the activities of users and system personnel within the application in greater detail. While the plan indicates the presence of these controls, the eCB security should provide adequate detail. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 135 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 178 |
| ***Guidance*** | Describe hardware or software features that are designed to permit only authorized access to or within the system to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists). | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 4.2 of the eCB security plan dated September 13, 2001 does software features designed to restrict access to the system. However, the security plan does not describe controls to restrict access once inside the system. | | |
| ***Recommendation*** | The eCB security plan should describe authorization controls within the system. While the authentication procedures are described adequately, authorization procedures should be addressed more thoroughly. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |

# Corrective Action Plan for the eCB System

| Finding | | | |
|---|---|---|---|
| ***Heading*** | MA-Technical Controls | ***Finding Number*** | 136 |
| ***Control*** | Logical Access Controls - MA | ***Id Number*** | 179 |
| ***Guidance*** | Does the security plan state the application has a standardized log-on banner? Is a copy of the banner provided? | | |
| ***Status*** | Somewhat Met | | |
| ***Review Assessment*** | Section 4.1 of the eCB security plan dated September 13, 2001 does state that the application has a standardized log-on banner, however a copy of the banner is not provided. Also, a "welcome page" should not be used, especially if a warning page is not posted first. | | |
| ***Recommendation*** | NIST 800-18, section 6.2, recommends that a security plan state that the application has a standardized log-on banner. SFA should post a warning banner in accordance with Public Law 99-474. Also, a copy of the new banner should be included in the security plan. | | |

| Corrective Action | | | | |
|---|---|---|---|---|
| ***Opinion*** | Concur | ☐ | Not Concur | ☐ |
| ***Corrective Action*** | | | | |
| ***POC*** | | | | |
| ***Estimated Completion Date*** | | ***Actual Completion Date*** | | |